15 November 2005

Net-centric Data Strategy:
Implementation Considerations

If the Joint Force fully exploits both shared knowledge and technical connectivity, the resulting capabilities will dramatically increase mission effectiveness and efficiency. This is the central idea behind creating a Network Centric Environment.

Net-Centric Environment Joint Functional Concept 1.0
07 April 2005

I. Introduction:

This paper is a scoping document highlighting some fundamental engineering considerations associated with the implementation of a network-centric data strategy within the Navy Enterprise. The Network Centric Environment Joint Functional Concept, the Global Information Grid, FORCEnet Functional Concepts and associated documents provide the framework for this paper.

Within context of the Navy's mission objectives, implementing Net-Centricity involves optimizing information resources across the warfighting domains. It creates an imperative for change and creates challenges that our current infrastructure cannot support. In 1999 DoN CIO established the Data Management and Interoperability IPT to address the growing data challenges then facing the department. At that time, data was (largely) developed, obtained and maintained by individual systems creating stovepipes of mission critical but non-interoperable data. The objective of the IPT was to identify and establish an enterprise approach to managing data, such that the Navy could create data once, share it across system boundaries, reduce the time required for decision-making, and avoid the cost of redundant efforts.[1]

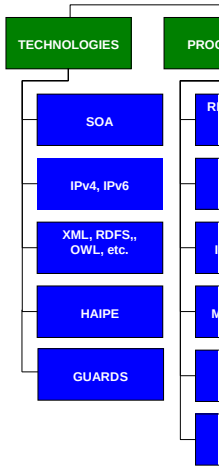
The IPT identified the problems and proposed solutions that ultimately resulted in the release of SECNAV instruction 5000.36 "Department of the Navy Data Management and Interoperability". Key themes emerging from the IPT were:

- Data problems are not unique to any one functional area or organization.
- There is a need for policy, process, supporting infrastructure, and a plan to leverage efforts.
- Data management requires senior management champions.
- Data management is not adequately addressed in budget or acquisition processes.

The problems and their associated solutions remain valid today. However, in the six years since the IPT was first convened, data interoperability has evolved from an important aspect of mission success to the central focus of DoD's Transformational Strategy. The introduction of new technologies coupled with the long term commitment by the Department of Defense to transform itself have created new opportunities and an imperative to define and implement rational approaches to these data sharing

challenges.

This paper is being presented at the FORCEnet Engineering Conference to stimulate acquisition community dialog. It is intended to support DoN CIO in the development of a Navy approach towards implementation of DoD Directive 8320.2 "Data Sharing in a Net-Centric Department of Defense".



Deleted:

II. Net-Centric Challenge: Managing Data within the Enterprise

There are dozens of policy directives, instructions and memoranda that relate to data. These policies are evolving rapidly as the technologies mature and the community's net-centric knowledge grows. A key step in developing a strategy in this dynamic environment is to articulate and scope the challenge properly.

As stated above, net-centricity is about reaching optimization of information resources across the Naval Enterprise, i.e., effectively exchanging, correlating, analyzing and reusing data throughout the various domains of the enterprise. This emerging global data-sharing (interoperability) requirement starts to change the way we think about the management of data. Key enabling concepts will need to be addressed as we begin to implement an Enterprise approach to data management, they include:

- Data ownership will no longer remain constant as data transverses (is used) throughout the enterprise.
- Data will be shared across the operational warfighting continuum and used by services/functions it was not initially intended to support creating an expanding group of data consumers not envisioned by the data producers.
- The visibility and accessibility of data across the enterprise will create an imperative that the Enterprise institutionalize and maintain designated authoritative data sources (i.e., data producers) to ensure trusted data sources.
- Stovepipe decisions effecting data generation by an individual data producer in the future will have a potentially negative effect on enterprise data needs.

Figure 1 depicts the major elements of the data strategy binned into five major categories. The major elements are based on a review of current DoD and Navy guidance. Parts of the data / information management infrastrucuture exist in various stages of maturity, however the roles and responsibilities associated with this new operating environment have not been fully codified.

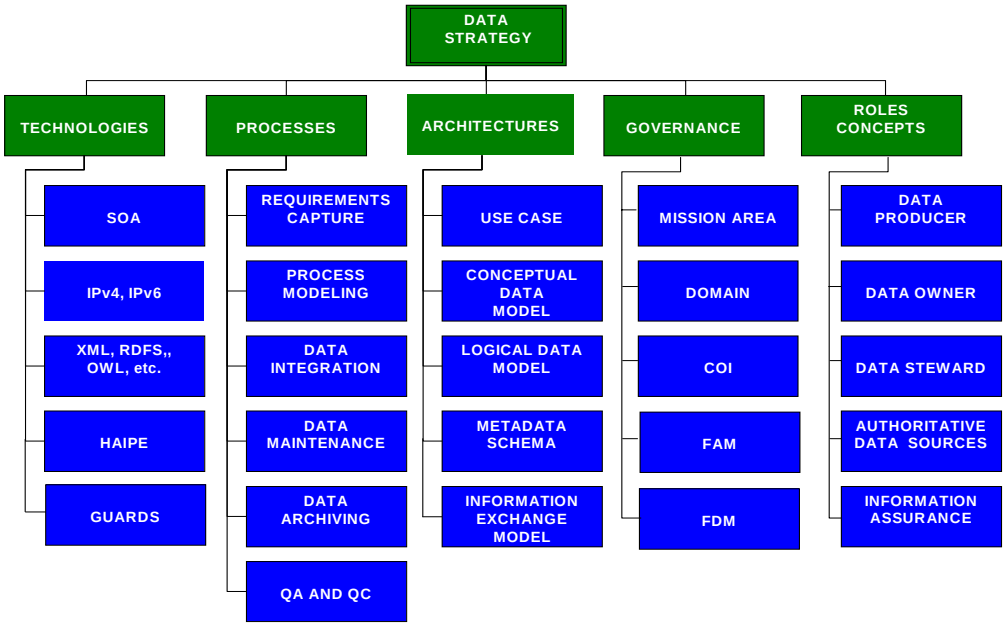


Figure 1: Data Strategy Elements

III. Technology

In order to appreciate the types of challenges and solutions that are possible, a brief description of the four basic technical tenets associated with DoD transformation is provided below. These tenets represent fundamental changes to the Information Technology infrastructure. The four major tenets are:

1. ***SOA:*** *Migrating to Services Oriented Architectures for application development.* In the past software applications were constructed as monolithic blocks that consisted of several tightly coupled layers (i.e., visualization, work flow logic, data). Modifications to any one of the layers affected the other layers. Since the data was designed for the specific application, it was not inherently sharable. Services Oriented Architectures are much more flexible and permit a tiered, loosely coupled implementation of the application layers. Often called an n-tier implementation, this means the visualization, workflow logic (services), and data tiers can be developed independently and more importantly, can be easily exposed for reuse. A graphical depiction of the concepts are shown in Figure 2.
2. ***Networks / Transport:*** *Migrating from circuit switched to packet switched networking (i.e., from tactical data links to IPV4 and IPV6 networks)* The major innovation with networks is the forced migration from circuit switched networks to IP or packet switched networks. IP based networking permits the scalability, flexibility and reach of the Internet. When coupled with a Services

Oriented Architecture, it permits a highly "distributed" environment in which services and data can be can be stored and managed in multiple locations then pulled and configured to support a mission requirement. SOA coupled with IP networking provides the infrastructure for "publish and subscribe" functionality from multiple locations simultaneously, configured and optimized. DoD's movement to IPV6 will (among other things) permit the expansion of the networking namespace. This will allow "every grain of sand" to have an IP address and therefore be discoverable on the network. The affect on data management is profound and is not yet fully explored within DoD literature.

3. ***Information Assurance:*** *Providing end-to-end security of the network, and providing assurance, confidentiality for data in transit and at rest potentially across multiple security domains.*
4. ***Data:*** *Making data visible, accessible and understandable on the network through meta tagging with the XML family of standards and posting to shared space.*

While the networks provide connectivity and services supply the application logic, capability improvements associated with the network centric environments lies largely in the fact that data assets can be made "smarter", can be loosely coupled to the other components of the infrastructure, and can be managed dynamically as a component of warfighter specified domains. Integration relates not to the level of interoperability of systems or applications but the ability of data to understand the meaning of, and it's relationship to, other data. Michael Daconta[2] discusses the evolution of data in terms of the "smart data continuum". Tagging of data with a metadata, registering the metadata, managing the data registries and defining authoritative data sources are all part of warfighting "data readiness".

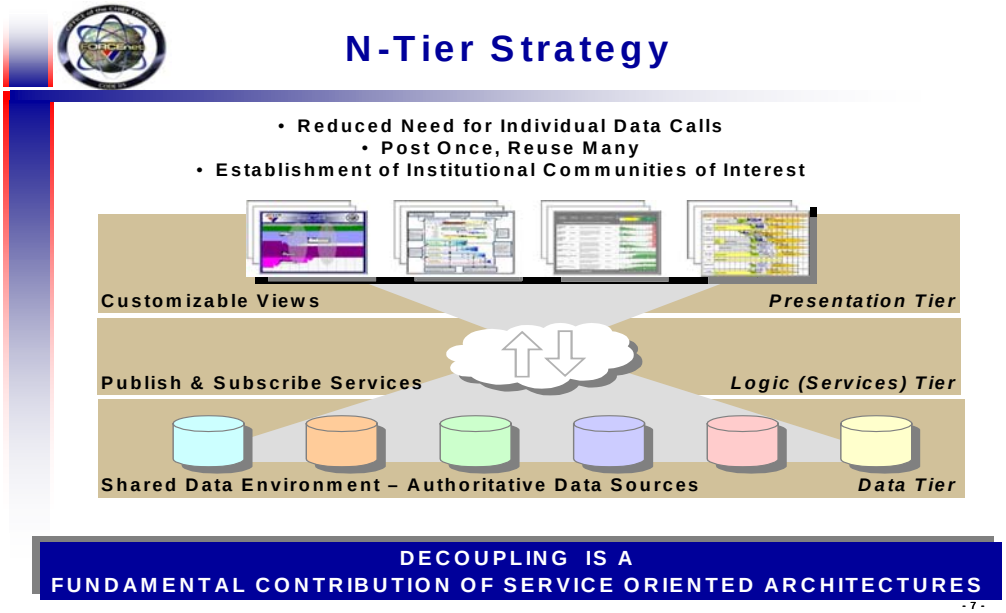


Figure 2: N-tier strategy

IV. Processes in Mission Context

An effective strategy involves the use of tailorable distributed web-services operating on smart data in a secure IP networking environment. Since data in a net-centric environment is loosely coupled to systems, applications and services, data attributes must be engineered directly into (or onto) the data and are not necessarily part of a database schema. The new data engineering techniques that permit increased capability also demand the implementation of sound metadata management processes and the implementation of rigorous data architectures.

JCS pub 6.0 describes seven criteria associated with the value of data. The DoD Net-centric Data Strategy uses slightly different, but consistent, concepts in its definitions of data goals. The list and abbreviated descriptions are annotated below. Data must be:

a. **Visible:** Discoverable or advertized on the network
b. **Accessible**: Stored in a shared space on the network
c. **Understandable**: Human and/or machine readable
d. **Trusted:** Relates to the authority and security of data
e. **Interoperable:** Many to many information exchanges at the data level
f. **Timely:** Available in time to make a decision
g. **Relevant:** As it applies to a specific mission
h. **Accurate:** The data conveys the truth at the required level of precision

Some of these data values can be achieved or improved through the effective creation, registration and management of metadata. Defined as data about data, metadata describes the characteristics of data and services such as content, quality, condition, producer, time. Metada permits users, humans and machines, to discover data and determine whether a data set (e.g., the content part of the data object) will meet their needs before it is processed**.**

Dialogue on data strategies often does not extend beyond this initial identification of a need to tag data. Metadata tagging alone is insufficient to achieve the stated quality goals and if improperly managed leads to data chaos. Metadata management is a subset of data architecting and engineering that addresses three major design elements (1) content, (2) structure, (3) context.

1. **Content:** A generic term used to describe information contained in files or web pages such as sound, text, images and video.
2. **Structure:** A logical relationship among data elements that is designed to support specific data manipulation functions. Includes schemas, data types, relational database constructs and file formats.
3. **Context:** The meaning of data. Context is provided syntactically (position and grammatical use) or semantically (i.e., comparisons and contrasts, definitions, descriptions, and the placement of new words near familiar words).

New data engineering techniques demand the modification of data management processes and the implementation of rigorous data architectures. These engineering technologies center on the development and management of the data requirements, guidelines, and procedures with mission completion serving as the unifying concept for

the data framework.

CJCSI 3170.01E, Joint Capabilities Integration and Development System, dated 11 May 2005, defines capability as " the ability to achieve desired effect under specified standards and conditions through combination of means and ways to perform a set of tasks." The combination of capabilities allows us to perform missions. Data must not only be interoperable but synchronized, synthesized, and exchanged as information across human and electronic interfaces from the systems level through the mission level. This means that a basic data stack exists similar to the OSI protocol stack with one layer interdependent with the other. A representation of the data stack is shown below in figure 3.

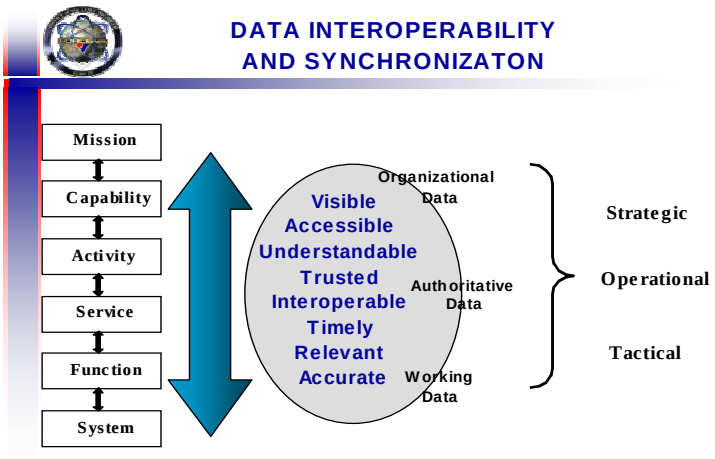


Figure 3: Data Interoperability and Synchronization

The seven criteria develop the context for transformation of data to information. Under FORCEnet, the data either becomes a net centric service or usable information for the human. The processing of data to achieve these seven information quality criteria is the essence of FORCEnet data engineering.

V. Data Architectures

The Department of Defense Architecture Framework (DODAF) assists with an understanding of our logical and physical data models. DODAF was sufficient for standardizing descriptions of these data models, but additional facets and views are necessary to realize the net-centric objectives for FORCEnet data. While logical and physical data models are important, they do not formalize and represent all of the data needs to ensure mission completion.

A formal conceptual model and conceptual data model is needed develop the common set of semantics about the data for mission completion. This means that our development of data architecture will leverage elements of DODAF, but also require the development of additional data views and aspects.

VI. Governance

The advent of Service Oriented Architectures and the imperative for publish / subscribe functionality resulted in a technical decoupling of data from specific systems and applications. The n-tier application environment and the shared data store concepts render traditional data governance in the Navy inadequate. Data governance relates to the responsibilities and authorities that must be executed in order to maximize information sharing. It involves moving away from system and application interfaces and toward interoperability at the data level. It also requires an Enterprise approach to management and oversight that encompasses old stovepipes and helps prevent the regrowth impermeable barriers between data domains.

Upon assuming command in July 2005, the Chief of Naval Operations, Admiral Mullen, tasked a review of the Single Provider Command concept.[2] The review resulted in recommendations to adopt an overarching Navy Enterprise construct, supported by Warfighter-led domains for balancing current readiness and future requirements".[4] This approach has practical implications for the management of data and data requirements.

Under the emerging construct there will be five overarching domains that make up the Naval Enterprise: Air, Ships, Submarines, Expeditionary Warfare and Networks. These domains will be tightly aligned with the provider commands and resource sponsors to maximize output at reduced cost[4]. Aligning the roles, responsibilities and authority for governance of data across this Enterprise and establishing the relationships between the Seapower 21 capability areas of Sea Strike, Basing, Shield, and Warrior is necessary for the successful implementation of net-centric data strategy.

Several organizational concepts have been co-evolving with DoD Transformation that are (or will be) part of the solution set for Navy's Enterprise Governance structure: Communities of Interest (COI), Functional Area Managers (FAM)/Functional Data Managers (FDM), DoD War Fighting Mission Areas and Portfolio Management.

Communities of Interest:
The DOD Net-centric Data Strategy and its policy corollary DODD 8320.2 define formal and informal constructs for managing data in a net-centric environment. Known collectively as Communities of Interest (COIs), they are defined as "users who must exchange information in pursuit of the mission and must therefore have a shared vocabulary for the information they exchange". COIs are divided into two fundamental categories: Expedient and Institutional.

For purposes of this paper, the more important of the categories are the Institutional COIs that provide the necessary foundational prerequisites data management, sharing and use. Institutional COIs conduct activities such as development of vocabularies, creating of logical data models, registration of community specific extensions to metadata schema. They also conduct other technical data related services and functions. One purpose of a Navy net-centric data strategy is to define the management, alignment and process for resourcing of the COIs. A reasonable approach is to align COIs within the emerging Joint mission areas.

Portfolio Management:
DoD Directive 8115.01, Information Technology Portfolio Management, dated October 10, 2005 defines an IT portfolio as "the grouping of IT investments by capability to accomplish a specific functional goal, objective or mission." The directive mandates the management of assigned portfolio management responsibilities to the War Fighting Mission Areas (WMA), Business Mission Area (BMA), the DoD portion of Intelligence Mission Area (DIMA), or the Enterprise Information Environment (EIE) Mission Area. The mission areas are responsible for the functions and processes that contribute to mission accomplishment. While not in the DoD Directive 8115.01, the mission areas are responsible for oversight of the Institutional COIs that affect their missions. Naval domain owner will be implementing various portfolio management mechanisms within their areas of responsibility. The DoN FAMs will report to the appropriate DoD Mission Areas for the accomplishment of DoN missions.

Functional Area Manager / Functional Data Manager:
The DoN established the Functional Area Managers (FAM) to oversee the applications on their networks. Functional area managers (FAMS) will have authority within their functional area and across echelon II organizational lines to: direct migration, consolidation, or retirement of applications and databases; develop and manage IT applications and database portfolios; and ensure technology strategies are aligned with business/administration processes and warfighting strategies.

The Functional Area Managers are generally the resource sponsors for the Navy and Marine Corps. The Navy has 23 FAMs and the Marine Corps has 16 FAMs. The Functional Data Managers (FDM) work for the FAMs. The FDMs serve as the portfolio managers for the FAMs and are designated in the SECNAV Inst. 5000.36a to designate the authoritative data sources. Per the SECNAV Inst 5000.36a, the FDMs are supposed to collect and manage the requirements for the authoritative data sources.

VII. Other Roles and Concepts

When data is tightly coupled to applications, system owners or programs are responsible for the associated data. The programs or systems are funded to manage the data as part of their development, operations and sustainment costs. Functional stovepipes provided fairly clear lanes of responsibility for shared data. In the net-centric environment, data is much more autonomous. The boundaries of domain or mission areas are also less clear. This autonomy creates challenges in management and resourcing and makes responsibility for the data across its lifecycle ambiguous.

Air Force Information and Data Management Strategy Policy provides insight into emerging roles and responsibilities in the net-centric data environment. Under Air Force policy, data owners are responsible for the "creation, collection, storage, release, and disposition of data". Data producers "exercise authority over data to include what data must be collected, how it is represented and stored, how it will be validated, the required degree of accuracy, precision and other quality factors, when it will be released and who is allowed to access it." If we superimpose these roles onto our navy infrastructure, it becomes clear that our current data management is not flexible enough to manage our data infrastructure at the enterprise, domain or mission area level. In addition, we will need to establish a new understanding concerning data roles:

Additionally, the Air Force strategy defines seven tasks for an organzational entity they

are calling a COI Data Panel. Navy data roles and responsibilities will have to be defined for similar tasks.

- Develop data priorities based on desired Capabilities
- Create a Subject-Area Vocabulary
- Maintain Inventories of Existing Data Assets
- Identify Authoritative Data Sources
- Prepare Integrated Data Access Plans
- Resolve Data Ownership Conflict
- Establish COI Data Processes

VIII. Summary

The Navy's data management challenges become more complex as our information sharing capabilities expand. Net-centric data management is on the Navy's transformation critical path. This paper framed the fundamental data problems identified by the Navy's Data Management and Interoperability IPT in terms of the capabilities and demands of operating in a network centric environment. It has described the emerging enterprise organization and the net-centric management constructs that will be required to operate effectively as the forces are transformed. The many facets of the data solution set were framed in terms of mission capability. Open and continuous community dialog on this critical topic will assisti Navy leadership in developing sound, executable net-centric data policy.

Dan Green
Dan.green@navy.mil

Paul Shaw
Paul.shaw@navy.mil

[1] Winters, Wilczynski. Data Interoperability: Foundation for Information Superiority. Chips. July 2000.
[2] Mr. Daconta is the metadata manager at the Department of Homeland Security and a globally recognized expert on data engineering technologies and the emerging Semantic Web.
[3] CNO Memorandum, Single Provider Command, of 25 July 2005
[4] From "Single Provider Command Recommendations". VADM Walter B. Massenburg Commander, Naval Air Systems Command, 05 October 2005.
[5] OPCIT CNO